CURRENT STATUS OF THE CLAIMS

1. (previously presented) A system for establishing a secure execution environment for a software process executed by a program operating on a computer, comprising:

a software process operating on a computer, said software process including a plurality of attributes;

an operating system kernel in communication with said software process and in communication with an executable file to be accessed by said software process; and

a system call trap associated with said operating system kernel, said system call trap configured to modify the plurality of attributes for the software process based on an executable environment attribute stored in association with said executable file.

2. (previously presented) The system of claim 1, wherein said system call trap further comprises:

a process attribute extension; and

an access token extension associated with said process attribute extension, said access token extension including said executable environment attribute.

3. (previously presented) The system of claim 1, wherein said executable environment attribute is contained in a database associated with said executable file.

4. (previously presented) The system of claim 1, wherein said executable environment attribute is chosen from the group consisting of user ID, group IDs and privileges.

5.   (original) The system of claim 1, wherein said execution environment isolates said software process from any other software process operating on said computer.

6.   (original) The system of claim 1, wherein said software process is a web server process.

7.   (original) The system of claim 1, wherein said software process is a file transfer process.

8.   (original) The system of claim 1, wherein said software process is a mail server process.

9.   (previously presented) The system of claim 1, wherein said executable environment attribute is associated to said software process upon execution of said software process.

10.   (previously presented) The system of claim 1, wherein said executable environment attribute replaces any existing attributes associated with said software process.

11.   (previously presented) A method for establishing a secure execution environment for a software process executed by a program operating on a computer, the method comprising:

operating a software process on a computer, said software process including a plurality of attributes;

executing an operating system kernel in communication with said software process, said operating system kernel in communication with an executable file to be accessed by said software process; and

modifying the plurality of attributes for the software process based on an executable environment attribute stored in association with the executable file.

12.   (previously presented) The method of claim 11, further comprising:

executing a process attribute extension; and

executing an access token extension associated with said process attribute extension, said access token extension including the executable environment attribute.

13.   (previously presented) The method of claim 11, wherein the executable environment attribute is contained in a database associated with said executable file.

14.   (previously presented) The method of claim 11, wherein said the executable environment attribute is chosen from the group consisting of user ID, group IDs and privileges.

15.   (original) The method of claim 11, wherein said execution environment isolates said software process from any other software process operating on said computer.

16.   (original) The method of claim 11, wherein said software process is a web server process.

17.   (original) The method of claim 11, wherein said software process is a file transfer process.

18.   (original) The method of claim 11, wherein said software process is a mail server process.

19.   (previously presented) The method of claim 11, wherein the executable environment attribute is associated to said software process upon execution of said software process.

20.   (previously presented) The method of claim 11, wherein the executable environment attribute replaces any existing attributes associated with said software process.

21.   (previously presented) A computer readable medium having a program for establishing a secure execution environment for a software process executed by a program operating on a computer, the program including logic for:

        operating a software process on a computer, said software process including a plurality of attributes;

        executing an operating system kernel in communication with said software process, said operating system kernel in communication with an executable file to be accessed by said software process; and

        modifying the plurality of attributes for the software process based on an executable environment attribute stored in association with the executable file.

22.   (previously presented) The program of claim 21, further comprising logic for:

executing a process attribute extension; and

executing an access token extension associated with said process attribute extension,

said access token extension including the executable environment attribute.

23.   (previously presented) The program of claim 21, wherein the executable environment

attribute is contained in a database associated with said executable file.

24.   (previously presented) The program of claim 21, wherein said the executable

environment attribute is chosen from the group consisting of user ID, group IDs and

privileges.

25.   (original) The program of claim 21, wherein said execution environment isolates said

software process from any other software process operating on said computer.

26.   (original) The program of claim 21, wherein said software process is a web server

process.

27.   (original) The program of claim 21, wherein said software process is a file transfer

process.

28.   (original) The program of claim 21, wherein said software process is a mail server

process.

29. (previously presented) The program of claim 21, wherein said the executable environment attribute is associated to said software process upon execution of said software process.

30. (previously presented) The program of claim 21, wherein the executable environment attribute replaces any existing attributes associated with said software process.

31. (previously presented) The system of claim 1, wherein the system call trap is further configured to determine whether the execution environment attribute contains an inherit flag.

32. (previously presented) The system of claim 31, wherein the system call trap is further configured to store a current attribute for a current process when the execution environment attribute contains an inherit flag.

33. (previously presented) The system of claim 32, wherein the system call trap is further configured to:

determine whether the current attribute for the current process contains the inherit flag;

merge the execution environment attribute with a previously stored attribute if the current attribute does not contain the inherit flag; and

merge the execution environment attribute with the current attribute if the current attribute does contain the inherit flag.

34. (previously presented) The method of claim 11, further comprising determining whether the execution environment attribute contains an inherit flag.

35.   (previously presented) The method of claim 34, further comprising storing a current attribute for a current process when the execution attribute contains an inherit flag.

36.   (previously presented) The method of claim 35, further comprising:

determining whether the current attribute for the current process contains the inherit flag; and

merging the execution environment attribute with a previously stored attribute if the current attribute does not contain the inherit flag.

37.   (previously presented) The method of claim 35, further comprising:

determining whether the current attribute for the current process contains the inherit flag; and

merging the execution environment attribute with the current attribute if the current attribute does contain the inherit flag.

38.   (previously presented) The computer readable medium of claim 21, further comprising logic for determining whether the execution environment attribute contains an inherit flag.

39.   (previously presented) The computer readable medium of claim 38, further comprising logic for storing a current attribute for a current process when the execution attribute contains an inherit flag.

40.   (previously presented) The computer readable medium of claim 39, further comprising logic for:

determining whether the current attribute for the current process contains the inherit flag;

merging the execution environment attribute with a previously stored attribute if the current attribute does not contain the inherit flag; and

merging the execution environment attribute with the current attribute if the current attribute does contain the inherit flag.